STATE OF TENNESSEE
DEPARTMENT OF FINANCE AND ADMINISTRATION

REQUEST FOR INFORMATION
FOR
SUPPLIER ACCOUNT VERIFICATION SERVICES

RFI # 31701-05046

July 1, 2021

1. STATEMENT OF PURPOSE:

The State of Tennessee, Department of Finance and Administration, Division of Accounts issues this Request for Information ("RFI") for the purpose of seeking knowledge from the vendor community regarding availability of Supplier Account Verification Services. We appreciate your input and participation in this process.

Information provided will assist the State in understanding the current state of the marketplace, including best practice for the industry approach to Supplier Account Verification Services.

2. BACKGROUND:

The Department of Finance and Administration, Division of Accounts currently processes approximately 500 bank account verifications each month using in-house human resources. In order to assist in reducing/mitigating payment fraud risks and accelerate the throughput of payment activities by expediting the enrollment of qualified suppliers, the State of Tennessee would like to implement an automated account verification solution that relies on account, transaction and other types of information from multiple reputable data sources. The state is also planning to utilize these services in conjunction with same-day ACH in order to fully maximize the state's use of the ACH network, and ultimately make faster and electronic payments to one time payees (an additional 4,000 transactions monthly) in a secure and low risk manner.

3. COMMUNICATIONS:

3.1. Please submit your response to this RFI, via e-mail, to:

Nichole.Stinnett@tn.gov

3.2. Please feel free to contact STS with any questions regarding this RFI. The main point of contact will be:

Nichole Stinnett
Department of Finance and Administration
312 Rosa L Parks Avenue, 19th Floor

Nashville, TN 37243
615-253-4416
Nichole.Stinnett@tn.gov

3.3. Please reference RFI # 31701-05046 with all communications to this RFI.

4. RFI SCHEDULE OF EVENTS:

EVENT		TIME (Central Time Zone)	DATE (all dates are State business days)
1.	RFI Issued		July 1, 2021
2.	Deadline for Respondent Questions	4:30 PM	July 8, 2021
3.	State Responds to Vendor Questions	4:30 PM	July 12, 3021
4.	RFI Response Deadline		July 16, 2021

5. GENERAL INFORMATION:

5.1. Please note that responding to this RFI is not a prerequisite for responding to any future solicitations related to this project and a response to this RFI will not create any contract rights. Responses to this RFI will become property of the State.

5.2. The information gathered during this RFI is part of an ongoing procurement. In order to prevent an unfair advantage among potential respondents, the RFI responses will not be available until after the completion of evaluation of any responses, proposals, or bids resulting from a Request for Qualifications, Request for Proposals, Invitation to Bid or other procurement method. In the event that the state chooses not to go further in the procurement process and responses are never evaluated, the responses to the procurement including the responses to the RFI, will be considered confidential by the State.

5.3. The State will not pay for any costs associated with responding to this RFI.

6. INFORMATIONAL FORMS:

The State is requesting the following information from all interested parties. Please fill out the following forms:

RFI #31701-03240 TECHNICAL INFORMATIONAL FORM
1. RESPONDENT LEGAL ENTITY NAME:
2. RESPONDENT CONTACT PERSON: Name, Title: Address: Phone Number: Email:
3. BRIEF DESCRIPTION OF EXPERIENCE PROVIDING SIMILAR SCOPE OF SERVICES/PRODUCTS:

Please describe, in the “Comments/Explanation” column, how your solution meets each requirement listed below:

Solution Requirements:

4. Requirement	Comments/Explanation
The ability to independently verify through an automated fashion supplier banking information, and, understand potential options for the storage and updating of supplier banking information, all in an effort to reduce the risk of payment fraud.	
The solution must verify the official account holder name	
The solution must verify the Tax ID of the supplier.	
The solution must verify the Bank routing number of the supplier.	
The solution must verify the Bank account number of the supplier.	
The solution must verify the Account type (Checking or savings) of the supplier.	
The solution must not require our suppliers to provide their bank's log-in credentials to verify their banking information.	
The hosting vendor should provide insurance to, or indemnify, its customers should an incorrect verification be provided and relied upon.	
The solution should verify the state's existing supplier's banking information.	

The solution should integrate with Oracle PeopleSoft (Edison).	
The solution should be supported by a mobile platform and multiple browser versions.	
The solution must be seamless for the supplier and not require any additional steps to the supplier registration process.	
The solution must verify information of new supplier onboarding as well as changes to existing suppliers.	
The solution must allow for online connection to their system to complete verification inquiries	
The vendor response of verification should be real time.	

Security Requirements.

5. Processing Capabilities:	**Comments/Explanation**
Standard security operating procedures and configurations should be documented, maintained and available to all users who need it.	
Change control procedures should include authorization, risk assessment, logging, audit ability, and roll back procedures.	
Development and testing environments should be segregated from production environments in order to reduce the risks of unauthorized access or changes to the production environment. Data classified as confidential must be protected from unauthorized	

disclosure, use, modification or destruction and should not be used in development or test environments.	
Should be protected from intentional or unintentional exposure to malicious software.	
Backup copies of data, software and system images should be taken and tested regularly in accordance with established procedures. A copy of the backup data should be stored off-site according to applicable regulatory requirements and State policy.	
Should be configured to support security event logging, recording user activities, exceptions, faults and information security events. System administrators should monitor and report inappropriate access to the STS Customer Care Center.	
Mission critical systems should be configured to support State approved automated monitoring of system availability and performance.	
Logging facilities and log information should be protected against tampering and unauthorized access	
System administrator activities should be logged and the logs protected and regularly reviewed.	
All applications and processing devices will have critical application, operating system, and/or security related patches made available by the software or hardware vendor applied within 90 calendar days or sooner if an acceptable date can be agreed upon by all affected parties. Emergency patches and updates will be applied	

as soon as possible following successful validation and testing. Patch schedule: · 14 days for critical patches addressing known exploits · 30 days for high patches addressing known exploits · 90 days for critical patches · 90 days high patches	
Server and workstation computing devices should have defined maintenance windows withing every 90 days. Appliances should have established review and maintenance cycles for software updates.	
All software is to be approved by STS and agency before install	
Access to the State of Tennessee's information resources will be granted consistent with the concept of least privilege. should have an appropriate role-based access control system that ensures only legitimate users and/or systems have access to data resources that they are explicitly authorized to use.	
Information security responsibilities should be defined and assigned by the access granting authority.	
A formal user registration and de-registration process should be available to enable assignment of access rights and to adjust those rights as the user's role changes.	
User accounts should be able to follow a State approved standardized naming convention	
A user's access rights should be reviewed, validated and updated for appropriate access by their section	

supervisor on a regular basis or whenever the user's access requirements change	
All access rights for employees and external entities to information and information processing facilities should be revoked upon termination of their employment, contract, agreement or change of agency by the close of business on the user's last working day.	
Where required by the access control policy, access to systems and application should be controlled by a secure log-on procedure. At a minimum, user access to protected information resources requires the utilization of User Identification (UserID) and password that uniquely identifies the user.	
Must display the State approved logon banner before the user is able to log in	
Access to program source code should be restricted to authorized users.	
Should be deployed with modified configurations for, but not limited to, default accounts, and/or installation paths to minimize the use of default settings to gain unauthorized use, modification or destruction.	
All passwords must contain a minimum of eight characters from the three of the following five categories: * Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic	

characters) * Lowercase characters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters) * Base 10 digits (0 through 9) * Non-alphanumeric characters: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/ * Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase. This includes Unicode characters from Asian languages.	
Passwords must be changed every 90 days or less from the last change.	
All systems that support password history will be configured to remember a password history of 4 at a minimum.	
All passwords should be hashed and salted.	
User ID's will be revoked after five (5) consecutive attempts to login with an invalid password.	
All service accounts should contain a minimum of 15 characters and meet 3 of the 5 categories listed above (O14)	
Inventory of all assets that are associated with information and information processing facilities should be created and maintained in order to protect the assets in accordance with Department of Finance and Administration Policy 32 Maintaining Control Over	

Items That Are Not Capitalized.	
An appropriate set of procedures for labeling data assets owned and/or managed by the State of Tennessee should be developed and implemented in accordance with the State's data classification scheme.	
Data classified as public should be protected from unauthorized modification or destruction.	
Data classified as confidential must be protected from unauthorized disclosure, use, modification or destruction and cannot be used in development or test environments or publicly disclosed. Controls should be applied to data in a manner consistent with its value, sensitivity and criticality to the business and operation of state government. Data classified as confidential must be encrypted at rest and during transmission in accordance with applicable state or federal statute or regulatory requirements.	
E-mail sent from the State's domain out through the public Internet must be encrypted if it contains confidential information in the body or attachment.	
Payment card information must be considered confidential when an individual's first name or first initial and last name are present in combination with account number, credit or debit card number, required security code, access code, or password that would permit access to an individual's financial account. All payment card information stored and processed by the State, or transmitted over State networks must be in	

compliance with the PCI-DSS.	
All workstation computing platforms, including all external storage devices, should be sanitized prior to being re-issued or re-purposed to another employee or outsourced employee.	
Agencies and full- and part-time employees of the State of Tennessee and all third parties, outsourced employees, or vendors who are acting on behalf of the State who use cloud services for State business should seek STS guidance and approval for proposed cloud solutions prior to enabling cloud services.	
Secure areas should be protected by appropriate entry controls to restrict access only to authorized personnel.	
Sessions will be configured to time out after 15 minutes of inactivity.	
Maximum inactivity interval for engaging screen-saver or other lockdown mechanism is 15 minutes.	
Security mechanisms, service levels and management requirements of all network services should be identified and included in network services agreements, whether these services are provided in-house or outsourced.	
Email and instant messages internal to the State's domain containing confidential data should be encrypted during transmission. Confidential information should not be placed into the subject line	

of email or as any part of instant messages.	
E-mail sent through the public Internet must be encrypted if it contains confidential information in the body or attachment of the email. Confidential information should not be placed into the subject line of the message.	
All electronic messages created, sent or received in conjunction with the transaction of official business should use the State approved gateway(s) to communicate via the Internet.	
Information and physical security requirements for mitigating the risks associated with supplier or vendor access to the State's assets should be agreed upon in writing with the external party. All external parties must agree in writing to comply with all applicable information security policies, confidentiality agreements, third party connectivity agreements, executive orders, standards, controls and regulations.	
All relevant information security requirements will be established and agreed upon with each supplier or vendor that may access, process, store, communicate, or provide IT infrastructure components for the State's processing systems or infrastructure.	
External Party Agreements will require external parties to report perceived security incidents that may impact the confidentiality, integrity or availability of State data immediately.	

Should not pass raw input to other processes including, but not limited to, other applications, web services, application server and databases. Applications should use parameterized queries or stored procedures, not dynamic SQL statements.	
Applications should not echo input back to the user or disclose information about the underlying system through error messages.	
Applications that provide access to information in databases or from network shares should perform user authentication.	
Should perform a Business Impact Analysis (BIA) to identify systems and infrastructure that are critical to State operations and services to citizens, other agencies and regulatory bodies.	
Procedures and controls should be established, documented and implemented to ensure the required level of business continuity during an adverse situation and reviewed at least annually.	
Employees and outsourced employees using the State's information systems and services are required to note and report any observed or suspected information security weaknesses in systems or services to the STS Customer Care Center.	
Information systems should protect the integrity of transmitted information traveling across both internal and external communications. This control applies to	

communications across internal and external networks	
Information systems should protect the confidentiality of transmitted information.	
The privacy and protection of personally identifiable information should be ensured as required by relevant federal or state statute or regulation.	
Employees and outsourced employees using the State's information systems and services are required to note and report any observed or suspected information security weaknesses in systems or services to the STS Customer Care Center.	

Please respond to the following sections:

COST INFORMATIONAL FORM ***Do NOT provide actual pricing***
1. Please list all services you provide.
2. Describe what pricing units / pricing structure you typically utilize for similar services or goods (e.g., per hour, per day, each, etc.) Please do **NOT** include specific pricing.

ADDITIONAL CONSIDERATIONS
1. Please provide input on alternative approaches or additional things to consider that might benefit the State: